Appendix B: Mapping Cybersecurity Assessment Tool to NIST Cybersecurity Framework

In 2014, the National Institute of Standards and Technology (NIST) released a Cybersecurity Framework for all sectors. The following provides a mapping of the FFIEC Cybersecurity Assessment Tool (Assessment) to the statements included in the NIST Cybersecurity Framework. NIST reviewed and provided input on the mapping to ensure consistency with Framework principles and to highlight the complementary nature of the two resources. As the Assessment is based on a number of declarative statements that address similar concepts across maturity levels, the mapping references the first time the concept arises beginning with the lowest maturity level. As such, statements at higher levels of maturity may also map to the NIST Cybersecurity Framework.

References for the NIST Cybersecurity Framework are provided by page number and, if applicable, by the reference code given to the statement by NIST. The Assessment declarative statements are referenced by location in the tool. Following the mapping is the guide to the development of the reference codes for the Assessment Tool.

The mapping is in the order of the NIST Cybersecurity Framework.

NIST Cybersecurity Framework	FFIEC Cybersecurity Assessment Tool
A clear understanding of the organization's business drivers and security considerations specific to use of informational technology and industrial control systems. (p. 4)	Accomplished by completing the Inherent Risk Profile part of the Assessment.
Describe current cybersecurity posture (p. 4)	Accomplished by completing the Cybersecurity Maturity part of the Assessment.
Describe target state for cybersecurity (p. 4)	Accomplished if an institution implements the Assessment as described in the User's Guide.
Identify and prioritize opportunities for improvement with the context of a continuous and repeatable process (p. 4)	Accomplished if an institution implements the Assessment as described in the User's Guide.
Assess progress toward the target state (p. 4)	Accomplished if an institution implements the Assessment as described in the User's Guide.
Communicate among internal and external stakeholders about cybersecurity risk (p. 4)	**D1.TC.Tr.B.3:** Situational awareness materials are made available to employees when prompted by highly visible cyber events or by regulatory alerts. **D1.TC.Tr.B.4:** Customer awareness materials are readily available (e.g., DHS' Cybersecurity Awareness Month materials).

Risk-based approach to managing cybersecurity risk (p. 4)	**D1.RM.RA.B.1:** A risk assessment focused on safeguarding customer information identifies reasonable and foreseeable internal and external threats, the likelihood and potential damage of threats and the sufficiency of policies, procedures and customer information systems. **D1.RM.RA.B.2:** The risk assessment identifies Internet-based systems and high-risk transactions that warrant additional authentication controls. **D1.RM.RA.B.3:** The risk assessment is updated to address new technologies, products, services, and connections before deployment.
Express a risk tolerance (p. 5)	**D1.G.Ov.Int.1:** The institution has a cyber risk appetite statement approved by the board or an appropriate board committee.
Determine how to handle risk (mitigate, transfer, avoid, accept) (p. 5)	Accomplished by completing the Cybersecurity Maturity part of the Assessment Tool.
Develop the organizational understanding to manage cybersecurity risk to systems, assets, data and capabilities (p. 8)	Accomplished by completing the Cybersecurity Maturity Domain 1, Assessment Factor Governance.
Develop and implement the appropriate safeguards to ensure delivery of critical infrastructure services (p. 8)	Accomplished by completing the Cybersecurity Maturity Domain 3, Assessment Factor Preventative Controls.
Develop and implement the appropriate activities to identify the occurrence of a cybersecurity event. (p. 8)	Accomplished by completing the Cybersecurity Maturity Domain 3, Assessment Factor Detective Controls, and Domain 5, Assessment Factor Detection, Response and Mitigation.
Develop and implement the appropriate activities to take action regarding a detected cybersecurity event. (p. 8)	Accomplished by completing the Cybersecurity Maturity Domain 5, Assessment Factor Detection, Response and Mitigation and Assessment Factor Escalation and Reporting.
Develop and implement the appropriate activities to maintain plans for resilience and to restore capabilities or services that were impaired due to a cybersecurity event. (p. 9)	Accomplished by completing the Cybersecurity Maturity Domain 5, Assessment Factor Incident Resilience Planning and Strategy.

Tier 1: Partial

NIST Cybersecurity Framework	FFIEC Cybersecurity Assessment Tool
Cybersecurity risk management is not formalized and risks are managed in an ad hoc and sometimes reactive manner. (p. 10)	This falls below Baseline.
Prioritization of cybersecurity activities may not be directly informed by organizational risk objectives, the threat environment or business/mission requirements. (p. 10)	This falls below Baseline.

NIST Cybersecurity Framework	FFIEC Cybersecurity Assessment Tool
Limited awareness of cybersecurity risk at the organizational level. (p. 10)	This falls below Baseline.
Organization-wide approach to managing cybersecurity risk has not been established. (p. 10)	This falls below Baseline.
Organization implements cybersecurity risk management on an irregular, case-by-case basis due to varied experience or information gained from outside sources. (p. 10)	This falls below Baseline.
Organization may not have processes that enable cybersecurity information to be shared within the organization. (p. 10)	This falls below Baseline.
Organization may not have the processes in place to participate in coordination or collaboration with other entities. (p. 10)	This falls below Baseline

Tier 2: Risk Informed

NIST Cybersecurity Framework	FFIEC Cybersecurity Assessment Tool
Risk management practices are approved by management but may not be established as organizational-wide policy. (p. 10)	**D1.RM.RMP.B.1:** An information security and business continuity risk management function(s) exists within the institution.
Prioritization of cybersecurity activities is directly informed by organizational risk objectives, the threat environment, or business/mission requirements. (p. 10)	**D2.TI.Th.B.3:** Threat information is used to enhance internal risk management and controls. **D1.G.Ov.Int.5:** The board or an appropriate board committee ensures management's annual cybersecurity self-assessment evaluates the institution's ability to meet its cyber risk management standards. **D1.G.SP.Int.2:** Management periodically reviews the cybersecurity strategy to address evolving cyber threats and changes to the institution's inherent risk profile.
There is an awareness of cybersecurity risk at the organizational level but an organization-wide approach to managing cybersecurity risk has not been established. (p. 10)	**D1.G.Ov.B.2:** Information security risks are discussed in management meetings when prompted by highly visible cyber events or regulatory alerts. **D1.TC.Tr.B.1:** Annual information security training is provided. **D1.TC.Tr.E.2:** Management is provided cybersecurity training relevant to their job responsibilities.
Risk-informed, management-approved processes and procedures are defined and implemented, and staff has adequate resources to perform their cybersecurity duties. (p. 10)	**D1.RM.RMP.E.1:** The risk management program incorporates cyber risk identification, measurement, mitigation, monitoring and reporting. **D1.R.St.E.3:** Staff with cybersecurity responsibilities have the requisite qualifications to perform the necessary tasks of the position.

Cybersecurity information is shared within the organization on an informal basis. (p. 10)	**D1.TC.Tr.B.3:** Situational awareness materials are made available to employees when prompted by highly visible cyber events or regulatory alerts.
The organization knows its role in the larger ecosystem, but has not formalized its capabilities to interact and share information externally. (p. 10)	**D1.G.SP.A.3:** The cybersecurity strategy identifies and communicates the institution's role as a component of critical infrastructure in the financial services industry. **D1.G.SP.Inn.1:** The cybersecurity strategy identifies and communicates the institution's role as it relates to other critical infrastructures. **D2.TI.Th.B.1:** The institution belongs or subscribes to a threat and vulnerability information-sharing source(s) that provides information on threats (e.g., FS-ISAC, US-CERT).

Tier 3: Repeatable

NIST Cybersecurity Framework	FFIEC Cybersecurity Assessment Tool
The organization's risk management practices are formally approved and expressed as policy. (p. 10)	**D1.G.SP.B.2:** The institution has policies commensurate with its risk and complexity that address the concepts of information technology risk management.
Organizational cybersecurity practices are regularly updated based on the application of risk management processes to changes in business/mission requirements and a changing threat and technology landscape. (p. 10)	**D1.G.SP.E.3:** A formal process is in place to update policies as the institution's inherent risk profile changes.
There is an organization-wide approach to manage cybersecurity risk. Risk-informed policies, processes, and procedures are defined, implemented as intended, and reviewed. (p. 10)	**D1.G.SP.Int.4:** Management links strategic cybersecurity objectives to tactical goals. **D1.G.RM.Au.B.1:** Independent audit or review evaluates policies, procedures, and controls across the institution for significant risks and control issues associated with the institution's operations, including risks in new products, emerging technologies, and information systems.
Consistent methods are in place to respond effectively to changes in risk. (p. 10)	**D1.G.SP.E.3:** A formal process is in place to update policies as the institution's inherent risk profile changes.
Personnel possess the knowledge and skills to perform their appointed roles and responsibilities. (p. 10)	**D1.R.St.E.2:** Management with appropriate knowledge and experience leads the institution's cybersecurity efforts. **D1.R.St.E.3:** Staff with cybersecurity responsibilities has the requisite qualifications to perform the necessary tasks of the position.

NIST Cybersecurity Framework	FFIEC Cybersecurity Assessment Tool
The organization understands its dependencies and partners and receives information from these partners that enables collaboration and risk-based management decisions within the organization in response to events. (p. 10)	**D4.C.Co.B.1:** The critical business processes that are dependent on external connectivity have been identified. **D2.TI.Th.B.1:** The institution belongs or subscribes to a threat and vulnerability information-sharing source(s) that provides information on threats (e.g., FS-ISAC, US-CERT). **D2.TI.Th.Int.1:** A formal threat intelligence program is implemented and includes subscription to threat feeds from external providers and internal sources. **D4.RM.Co.E.2:** Responsibility for notification of direct and indirect security incidents and vulnerabilities is documented in contracts or SLAs.

Tier 4: Adaptive

NIST Cybersecurity Framework	FFIEC Cybersecurity Assessment Tool
Adapt cybersecurity practices based on lessons learned and predictive indicators derived from previous and current cybersecurity activities. (p. 11)	**D5.DE.Re.E.8:** Analysis of events is used to improve the institution's security measures and policies. **D5.IR.Pl.Int.4:** Lessons learned from real-life cyber incidents and attacks on the institution and other organizations are used to improve the institution's risk mitigation capabilities and response plan. **D1.TC.Tr.Int.1:** Management incorporates lessons learned from social engineering and phishing exercises to improve the employee awareness programs.
Continually incorporates advanced technologies and practices, adapting to a changing cybersecurity landscape. (p. 11)	**D1.G.SP.A.5:** Management is continuously improving the existing cybersecurity program to adapt as the desired cybersecurity target state changes.
Responds to evolving and sophisticated threats in a timely manner. (p. 11)	**D5.IR.Pl.B.1:** The institution has documented how it will react and respond to cyber incidents. **D5.IR.Pl.A.2:** Multiple systems, programs, or processes are implemented into a comprehensive cyber resilience program to sustain, minimize and recover operations from an array of potentially disruptive and destructive cyber incidents.

NIST Cybersecurity Framework	FFIEC Cybersecurity Assessment Tool
Manages cybersecurity risk through an organization-wide approach using risk-informed policies, processes, and procedures to address potential cybersecurity events. (p. 11)	**D5.IR.Pl.B.1:** The institution has documented how it will react and respond to cyber incidents **D1.TC.Cu.E.1:** The institution has formal standards of conduct that hold all employees accountable for complying with all cybersecurity policies and procedures. **D1.RM.RMP.Int.2:** The risk management program specifically addresses cyber risks beyond the boundaries of the technological impacts (e.g., financial, strategic, regulatory, compliance). **D1.G.Ov.A.5:** Management and the board or an appropriate board committee hold business units accountable for effectively managing all cyber risks associated with their activities.
Encourage cybersecurity risk management as part of culture. (p. 11)	**D1.TC.Cu.Int.2:** The risk culture requires formal consideration of cyber risks in all business decisions. **D1.TC.Cu.A.1:** Management ensures continuous improvement of cyber risk cultural awareness.
Evolve process from an awareness of previous activities, information shared by other sources, and continuous awareness of activities on systems and networks. (p. 11)	**D1.G.Ov.A.2:** Management has a formal process to continuously improve cybersecurity oversight.
Actively share information with partners to ensure that accurate, current information is being distributed and consumed to improve cybersecurity before a cybersecurity event occurs. (p. 11)	**D2.IS.Is.Int.3:** Information is shared proactively with the industry, law enforcement, regulators, and information-sharing forums.

Framework Profile

NIST Cybersecurity Framework	FFIEC Cybersecurity Assessment Tool
Establish a roadmap for reducing cybersecurity risk. (p. 11)	Accomplished if an institution implements the Assessment as described in the User's Guide.
Develop a current profile. (p. 11)	Accomplished if an institution implements the Assessment as described in the User's Guide.
Develop a target profile. (p. 11)	Accomplished if an institution implements the Assessment as described in the User's Guide.
Identify and remediate gaps in current and target profiles. (p. 11)	Accomplished if an institution implements the Assessment as described in the User's Guide.
Develop a risk-management approach to achieve cybersecurity goals in a cost-effective, prioritized manner (p. 11)	Discussed in the User's Guide.
Executive leadership communicates the mission priorities, available resources, and overall risk tolerance to the business/process level. (p. 12)	Discussed in the User's Guide and the Overview for Chief Executive Officers and Boards of Directors.

NIST Cybersecurity Framework	FFIEC Cybersecurity Assessment Tool
Business/Process managers collaborate with the implementation/operations level to communicate business needs and create a risk profile using the input from the executive leadership. (p. 12)	Discussed in the User's Guide and the Overview for Chief Executive Officers and Boards of Directors.
Business/process managers perform an impact assessment from the implementation progress provided by the implementation/operations group. (p. 12)	Discussed in the User's Guide and the Overview for Chief Executive Officers and Boards of Directors.
Business/process managers perform an impact assessment from the implementation progress provided by the implementation/operations group. (p. 12)	Discussed in the User's Guide and the Overview for Chief Executive Officers and Boards of Directors.
Business/process managers report the outcomes of that impact assessment to the executive level to inform the organization's overall risk management process. (p. 12)	Discussed in the User's Guide and the Overview for Chief Executive Officers and Boards of Directors.
Business/process managers notify the implementation/operations level to raise awareness of business impact. (p. 12)	Discussed in the User's Guide and the Overview for Chief Executive Officers and Boards of Directors.
Operations group communicates the risk Profile implementation progress to the business/process level. (p. 12)	Discussed in the User's Guide and the Overview for Chief Executive Officers and Boards of Directors.
Create or improve a cybersecurity program. (p. 13)	Discussed in the User's guide.
Organization identifies its business/mission objectives and high-level organizational priorities. (p. 14)	Discussed in the User's guide.
Organization identifies related systems and assets, regulatory requirements, and overall risk approach. (p. 14)	Accomplished by completing the Inherent Risk Profile part of the Tool.
Organization identifies threats to, and vulnerabilities of, identified systems and assets (p. 14)	Accomplished if an institution completes the Inherent Risk Profile part of the Assessment.
Develop a current profile. (p. 14)	Accomplished if an institution implements the Assessment as described in the User's Guide.
Conduct a risk assessment. (p. 14)	Accomplished if an institution completes the Inherent Risk Profile part of the Assessment.
Create a target profile. (p. 14)	Accomplished if an institution implements the Assessment as described in the User's Guide.
Compare the current and target profile to determine gaps. (p. 14)	Accomplished if an institution implements the Assessment as described in the User's Guide.
Create a prioritized action plan to address gaps. (p. 14)	Accomplished if an institution implements the Assessment as described in the User's Guide.
Implement action plan. (p. 14)	Accomplished if an institution implements the Assessment as described in the User's Guide.

NIST Cybersecurity Framework	FFIEC Cybersecurity Assessment Tool
Repeat as needed to continuously assess and improve cybersecurity. (p. 14)	Accomplished if an institution implements the Assessment as described in the User's Guide.
Communicate cybersecurity requirements with interdependent stakeholders responsible for the delivery of essential critical infrastructure services. (p. 15)	**D4.RM.Co.B.1:** Formal contracts that address relevant security and privacy requirements are in place for all third parties that process, store, or transmit confidential data or provide critical services. **D4.RM.Co.E.2:** Responsibility for notification of direct and indirect security incidents and vulnerabilities is documented in contracts or SLAs.
Identify and address individual privacy and civil liberties implications that may result from cybersecurity operations (p. 15) Governance of cybersecurity risk. Identifying and authorizing access. Awareness and training measures. Anomalous activity detection reviewed for privacy concerns. Review of the sharing of personal information within and outside of the organization.	**D4.RM.Co.B.1:** Formal contracts that address relevant security and privacy requirements are in place for all third parties that process, store, or transmit confidential data or provide critical services. **D1.G.Ov.E.2:** Management is responsible for ensuring compliance with legal and regulatory requirements related to cybersecurity. **D2.IS.Int.2:** Information-sharing agreements are used as needed or required to facilitate sharing threat information with other financial sector institutions or third parties.

Appendix A: Framework Core

NIST Cybersecurity Framework	FFIEC Cybersecurity Assessment Tool
ID.AM-1: Physical devices and systems within the organization are inventoried. (p. 20)	**D1.G.IT.B.1:** An inventory of organizational assets (e.g., hardware, software, data, and systems hosted externally) is maintained.
ID.AM-2: Software platforms and applications within the organization are inventoried. (p. 20)	**D1.G.IT.B.1:** An inventory of organizational assets (e.g., hardware, software, data, and systems hosted externally) is maintained.
ID.AM-3: The organizational communication and data flow is mapped. (p. 20)	**D4.C.Co.B.4:** Data flow diagrams are in place and document information flow to external parties. **D4.C.Co.Int.1:** A validated asset inventory is used to create comprehensive diagrams depicting data repositories, data flow, infrastructure, and connectivity.
ID.AM-4: External information systems are mapped and catalogued. (p. 20)	**D4.RM.Dd.B.2:** A list of third-party service providers is maintained. **D4.C.Co.B.3:** A network diagram is in place and identifies all external connections.
ID.AM-5: Resources are prioritized based on the classification / criticality / business value of hardware, devices, data, and software. (p. 20)	**D1.G.IT.B.2:** Institution assets (e.g., hardware, systems, data, and applications) are prioritized for protection based on the data classification and business value.
ID.AM-6: Workforce roles and responsibilities for business functions, including cybersecurity, are established. (p. 20)	**D1.R.St.B.1:** Information security roles and responsibilities have been identified. **D1.TC.Cu.B.1:** Management holds employees accountable for complying with the information security program.
ID.BE-1: The organization's role in the supply chain is identified and communicated. (p. 21)	**D1.G.SP.A.3:** The cybersecurity strategy identifies and communicates the institution's role as a component of critical infrastructure in the financial services industry.
ID.BE-2: The organization's place in critical infrastructure and their industry ecosystem is identified and communicated. (p. 21)	**D1.G.SP.Inn.1:** The cybersecurity strategy identifies and communicates its role as it relates to other critical infrastructures.
ID.BE-3: Priorities for organizational mission, objectives, and activities are established. (p. 21)	**D1.G.SP.E.2:** The institution has a formal cybersecurity program that is based on technology and security industry standards or benchmarks. **D1.G.Ov.Int.5:** The board or an appropriate board committee ensures management's annual cybersecurity self-assessment evaluates the institution's ability to meet its cyber risk management standards. **D1.G.SP.Int.3:** The cybersecurity strategy is incorporated into, or conceptually fits within, the institution's enterprise-wide risk management strategy.

NIST Cybersecurity Framework	FFIEC Cybersecurity Assessment Tool
ID.BE-4: Dependencies and critical functions for delivery of critical services are established. (p. 21)	**D4.C.Co.B.1:** The critical business processes that are dependent on external connectivity have been identified. **D1.G.IT.B.2:** Organizational assets (e.g., hardware, systems, data, and applications) are prioritized for protection based on the data classification and business value.
ID.BE-5: Resilience requirements to support delivery of critical services are established. (p. 21)	**D5.IR.Pl.B.5:** A formal backup and recovery plan exists for all critical business lines. **D5.IR.Pl.E.3:** Alternative processes have been established to continue critical activity within a reasonable time period.
ID.GV-1: Organizational information security policy is established. (p. 21)	**D1.G.Ov.SP.B.4:** The institution has board-approved policies commensurate with its risk and complexity that address information security.
ID.GV-2: Information security roles & responsibility are coordinated and aligned with internal roles and external partners. (p. 21)	**D1.G.Ov.SP.B.7:** All elements of the information security program are coordinated enterprise-wide. **D4.RM.Co.B.2:** Contracts acknowledge that the third party is responsible for the security of the institution's confidential data that it possesses, stores, processes, or transmits. **D4.RM.Co.B.5:** Contracts establish responsibilities for responding to security incidents.
ID.GV-3: Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed. (p. 21)	**D1.G.Ov.E.2:** Management is responsible for ensuring compliance with legal and regulatory requirements related to cybersecurity.
ID.GV-4: Governance and risk management processes address cybersecurity risks. (p. 22)	**D1.G.Ov.B.1:** Designated members of management are held accountable by the board or an appropriate board committee for implementing and managing the information security and business continuity programs. **D1.G.Ov.B.3:** Management provides a written report on the overall status of the information security and business continuity programs to the board or an appropriate committee of the board at least annually. **D1.G.Ov.E.1:** At least annually, the board or an appropriate board committee reviews and approves the institution's cybersecurity program. **D1.G.SP.E.1:** The institution augmented its information security strategy to incorporate cybersecurity and resilience. **D1.G.Ov.Int.1:** The institution has a cyber risk appetite statement approved by the board or an appropriate board committee.

NIST Cybersecurity Framework	FFIEC Cybersecurity Assessment Tool
ID.RA-1: Asset vulnerabilities are identified and documented. (p. 22)	**D2.TI.Ti.B.2:** Threat information is used to monitor threats and vulnerabilities. **D3.DC.Th.B.1:** Independent testing (including penetration testing and vulnerability scanning) is conducted according to the risk assessment for the external-facing systems and the internal network. **D1.RM.RA.E.2:** The focus of the risk assessment has expanded beyond customer information to address all information assets. **D3.DC.Th.E.5:** Vulnerability scanning is conducted and analyzed before deployment/redeployment of new/existing devices. **D3.DC.Th.A.1:** Weekly vulnerability scanning is rotated amongst environments to scan all environments throughout the year.
ID.RA-2: Threat and vulnerability information is received from information-sharing forums and sources. (p. 22)	**D2.TI.Ti.B.1:** The institution belongs or subscribes to a threat and vulnerability information-sharing source(s) that provides information on threats (e.g., FS-ISAC, US-CERT).
ID.RA-3: Threats to organizational assets are identified and documented. (p. 22)	**D3.DC.An.B.1:** The institution is able to detect anomalous activities through monitoring across the environment. **D2.MA.Ma.E.1:** A process is implemented to monitor threat information to discover emerging threats. **D2.MA.Ma.E.4:** Monitoring systems operate continuously with adequate support for efficient incident handling. **D2.MA.Ma.Int.2:** A profile is created for each threat that identifies the likely intent, capability, and target of the threat.
ID.RA-4: Potential impacts are analyzed. (p. 22)	**D5.RE.Re.B.1:** Appropriate steps are taken to contain and control an incident to prevent further unauthorized access to or use of customer information. **D5.ER.Er.Ev.1:** Criteria have been established for escalating cyber incidents or vulnerabilities to the board and senior management based on the potential impact and criticality of the risk.
ID.RA-5: Threats, vulnerabilities, likelihoods, and impacts are used to determine risk. (p. 22)	**D1.RM.RA.B.1:** A risk assessment focused on safeguarding customer information identifies reasonable and foreseeable internal and external threats, the likelihood and potential damage of threats, and the sufficiency of policies, procedures and customer information systems. **D1.RM.RA.E.2:** The focus of the risk assessment has expanded beyond customer information to address all information assets. **D1.RM.RA.E.1:** Risk assessments are used to identify the cybersecurity risks stemming from new products, services, or relationships.

NIST Cybersecurity Framework	FFIEC Cybersecurity Assessment Tool
ID.RA-6: Risk responses are identified and prioritized. (p. 22)	**D5.IR.Pl.B.1:** The institution has documented how it will react and respond to cyber incidents. **D5.DR.Re.E.1:** The incident response plan is designed to prioritize incidents, enabling a rapid response for significant cybersecurity incidents or vulnerabilities. **D5.IR.Pl.E.1:** The remediation plan and process outlines the mitigating actions, resources, and time parameters.
ID.RM-1: Risk management processes are managed and agreed to by organizational stakeholders. (p. 23)	**D1.G.Ov.B.1:** Designated members of management are held accountable by the board or an appropriate board committee for implementing and managing the information security and business continuity programs.
ID.RM-2: Organizational risk tolerance is determined and clearly expressed. (p. 23)	**D1.G.Ov.Int.3:** The institution has a cyber risk appetite statement approved by the board or an appropriate board committee.
ID.RM-3: The organization's determination of risk tolerance is informed by their role in critical infrastructure and sector specific risk analysis. (p. 23)	**D1.G.SP.A.4:** The risk appetite is informed by the institution's role in critical infrastructure.
PR.AC-1: Identities and credentials are managed for authorized devices and users. (p. 23)	**D3.PC.Im.B.7:** Access to make changes to systems configurations (including virtual machines and hypervisors) is controlled and monitored. **D3.PC.Am.B.6:** Identification and authentication are required and managed for access to systems, applications, and hardware.
PR.AC-2: Physical access to assets is managed and protected. (p. 23)	**D3.PC.Am.B.11:** Physical security controls are used to prevent unauthorized access to information systems and telecommunication systems. **D3.PC.Am.B.17:** Administrative, physical, or technical controls are in place to prevent users without administrative responsibilities from installing unauthorized software.
PR.AC-3: Remote access is managed. (p. 23)	**D3.PC.Am.B.15:** Remote access to critical systems by employees, contractors, and third parties uses encrypted connections and multifactor authentication. **D3.PC.De.E.7:** The institution wipes data remotely on mobile devices when a device is missing or stolen. (*N/A if mobile devices are not used.) **D3.PC.Im.Int.2:** Security controls are used for remote access to all administrative consoles, including restricted virtual systems.

NIST Cybersecurity Framework	FFIEC Cybersecurity Assessment Tool
PR.AC-4: Access permissions are managed, incorporating the principles of least privilege and separation of duties. (p. 24)	**D3.PC.Am.B.1:** Employee access is granted to systems and confidential data based on job responsibilities and the principles of least privilege. **D3.PC.Am.B.2:** Employee access to systems and confidential data provides for separation of duties. **D3.PC.Am.B.5:** Changes to physical and logical user access, including those that result from voluntary and involuntary terminations, are submitted to and approved by appropriate personnel.
PR.AC-5: Network integrity is protected, incorporating network segregation where appropriate. (p. 24)	**D3.DC.Im.B.1:** Network perimeter defense tools (e.g., border router and firewall) are used. **D3.DC.Im.Int.1:** The enterprise network is segmented in multiple, separate trust/security zones with defense-in-depth strategies (e.g., logical network segmentation, hard backups, air-gapping) to mitigate attacks.
PR.AT-1: All users are informed and trained. (p. 24)	**D1.TC.Tr.B.2:** Annual information security training includes incident response, current cyber threats (e.g., phishing, spear phishing, social engineering, and mobile security), and emerging issues.
PR.AT-2: Privileged users understand roles & responsibilities. (p. 24)	**D1.TC.Tr.E.3:** Employees with privileged account permissions receive additional cybersecurity training commensurate with their levels of responsibility.
PR.AT-3: Third-party stakeholders (suppliers, customers, partners) understand roles & responsibilities. (p. 24)	**D1.TC.Tr.B.4:** Customer awareness materials are readily available (e.g., DHS' Cybersecurity Awareness Month materials). **D1.TC.Tr.Int.2:** Cybersecurity awareness information is provided to retail customers and commercial clients at least annually.
PR.AT-4: Senior executives understand roles and responsibilities. (p. 24)	**D1.TC.Tr.E.2:** Management is provided cybersecurity training relevant to their job responsibilities.
PR.AT-5: Physical and information security personnel understand roles & responsibilities. (p. 25)	**D1.TC.Tr.E.3:** Employees with privileged account permissions receive additional cybersecurity training commensurate with their levels of responsibility. **D1.R.St.E.3:** Staff with cybersecurity responsibilities has the requisite qualifications to perform the necessary tasks of the position.

NIST Cybersecurity Framework	FFIEC Cybersecurity Assessment Tool
PR.DS-1: Data-at-rest is protected. (p. 25)	**D1.G.IT.B.13:** Confidential data is identified on the institution's network. **D3.PC.Am.B.14:** Mobile devices (e.g., laptops, tablets, and removable media) are encrypted if used to store confidential data. (*N/A if mobile devices are not used). **D4.RM.Co.B.1:** Formal contracts that address relevant security and privacy requirements are in place for all third parties that process, store, or transmit confidential data or provide critical services. **D3.PC.Am.A.1:** Encryption of select data at rest is determined by the institution's data classification and risk assessment.
PR.DS-2: Data-in-transit is protected. (p. 25)	**D3.PC.Am.B.13:** Confidential data is encrypted when transmitted across public or untrusted networks (e.g., Internet). **D3.PC.Am.E.5:** Controls are in place to prevent unauthorized access to cryptographic keys. **D3.PC.Am.Int.7:** Confidential data is encrypted in transit across private connections (e.g., frame relay and T1) and within the institution's trusted zones.
PR.DS-3: Assets are formally managed throughout removal, transfers, and disposition. (p. 25)	**D1.G.IT.E.3:** The institution proactively manages system end-of-life (e.g., replacement) to limit security risks. **D1.G.IT.E.2:** The institution has a documented asset life-cycle process that considers whether assets to be acquired have appropriate security safeguards.
PR.DS-4: Adequate capacity to ensure availability is maintained. (p. 25)	**D5.IR.Pl.B.5:** A formal backup and recovery plan exists for all critical business lines. **D5.IR.Pl.B.6:** The institution plans to use business continuity, disaster recovery, and data backup programs to recover operations following an incident. **D5.IR.Pl.E.3:** Alternative processes have been established to continue critical activity within a reasonable time period. **D3.PC.Im.E.4:** A risk-based solution is in place at the institution or Internet-hosting provider to mitigate disruptive cyber attacks (e.g., DDoS attacks).

NIST Cybersecurity Framework	FFIEC Cybersecurity Assessment Tool
PR.DS-5: Protections against data leaks are implemented. (p. 26)	**D3.PC.Am.B.15:** Remote access to critical systems by employees, contractors, and third parties uses encrypted connections and multifactor authentication. **D3.PC.Am.Int.1:** The institution has implemented tools to prevent unauthorized access to or exfiltration of confidential data. **D3.PC.De.Int.1:** Data loss prevention controls or devices are implemented for inbound and outbound communications (e.g., e-mail, FTP, Telnet, prevention of large file transfers). **D3.DC.Ev.Int.1:** Controls or tools (e.g., data loss prevention) are in place to detect potential unauthorized or unintentional transmissions of confidential data.
PR.DS-6: Integrity checking mechanisms are used to verify software, firmware, and information integrity. (p. 26)	**D3.PC.Se.Int.3:** Software code executables and scripts are digitally signed to confirm the software author and guarantee that the code has not been altered or corrupted. **D3.PC.De.Int.2:** Mobile device management includes integrity scanning (e.g., jailbreak/rooted detection). (*N/A if mobile devices are not used.)
PR.DS-7: The development and testing environment(s) are separate from the production environment. (p. 26)	**D3.PC.Am.B.10:** Production and non-production environments are segregated to prevent unauthorized access or changes to information assets. (*N/A if no production environment exists at the institution or the institution's third party.)
PR.IP-1: A baseline configuration of information technology/industrial control systems is created and maintained. (p. 26)	**D3.PC.Im.B.5:** Systems configurations (for servers, desktops, routers, etc.) follow industry standards and are enforced.
PR.IP-2: A System Development Life Cycle to manage systems is implemented. (p. 26)	**D3.PC.Se.B.1:** Developers working for the institution follow secure program coding practices, as part of a system development life cycle (SDLC), that meet industry standards. **D3.PC.Se.E.1:** Security testing occurs at all post-design phases of the SDLC for all applications, including mobile applications. (*N/A if there is no software development.)
PR.IP-3: Configuration change control processes are in place. (p. 27)	**D1.G.IT.B.4:** A change management process is in place to request and approve changes to systems configurations, hardware, software, applications, and security tools.
PR.IP-4: Backups of information are conducted, maintained, and tested periodically. (p. 27)	**D5.IR.Pl.B.5:** A formal backup and recovery plan exists for all critical business lines. **D5.IR.Te.E.3:** Information backups are tested periodically to verify they are accessible and readable.
PR.IP-5: Policy and regulations regarding the physical operating environment for organizational assets are met. (p. 27)	**D3.PC.Am.B.11:** Physical security controls are used to prevent unauthorized access to information systems and telecommunication systems.

NIST Cybersecurity Framework	FFIEC Cybersecurity Assessment Tool
PR.IP-6: Data is destroyed according to policy. (p. 27)	**D1.G.IT.B.19:** Data is disposed of or destroyed according to documented requirements and within expected time frames.
PR.IP-7: Protection processes are continuously improved. (p. 27)	**D1.RM.RMP.E.2:** Management reviews and uses the results of audits to improve existing policies, procedures, and controls. **D1.G.Ov.A.2:** Management has a formal process to continuously improve cybersecurity oversight.
PR.IP-8: Effectiveness of protection technologies is shared with appropriate parties. (p. 28)	**D2.IS.Is.B.1:** Information security threats are gathered and shared with applicable internal employees. **D.2.IS.Is.E.2:** A representative from the institution participates in law enforcement or information-sharing organization meetings.
PR.IP-9: Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed. (p. 28)	**D5.IR.Pl.B.1:** The institution has documented how it will react and respond to cyber incidents.
PR.IP-10: Response and recovery plans are tested. (p. 28)	**D5.IR.Te.B.1:** Scenarios are used to improve incident detection and response. **D5.IR.Te.B.3:** Systems, applications, and data recovery is tested at least annually.
PR.IP-11: Cybersecurity is included in human resources practices (e.g., deprovisioning, personnel screening). (p. 28)	**D1.R.St.E.4:** Employment candidates, contractors, and third parties are subject to background verification proportional to the confidentiality of the data accessed, business requirements, and acceptable risk.
PR.IP-12: A vulnerability management plan is developed and implemented. (p. 28**)**	**D3.CC.Re.Ev.2:** Formal processes are in place to resolve weaknesses identified during penetration testing.
PR.MA-1: Maintenance and repair of organizational assets is performed and logged in a timely manner, with approved and controlled tools (p. 28)	**D3.CC.Re.Int.5:** The maintenance and repair of organizational assets are performed by authorized individuals with approved and controlled tools. **D3.CC.Re.Int.6:** The maintenance and repair of organizational assets are logged in a timely manner.
PR.MA-2: Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access (p. 28)	**D3.PC.Im.B.7:** Access to make changes to systems configurations (including virtual machines and hypervisors) is controlled and monitored.
PR.PT-1: Audit/log records are determined, documented, implemented, and reviewed in accordance with policy. (p. 29)	**D1.G.SP.B.3:** The institution has policies commensurate with its risk and complexity that address the concepts of threat information sharing. **D2.MA.Ma.B.1:** Audit log records and other security event logs are reviewed and retained in a secure manner. **D2.MA.Ma.B.2:** Computer event logs are used for investigations once an event has occurred.

NIST Cybersecurity Framework	FFIEC Cybersecurity Assessment Tool
PR.PT-2: Removable media is protected and its use restricted according to a specified policy. (p. 29)	**D1.G.SP.B.4:** The institution has board-approved policies commensurate with its risk and complexity that address information security. **D3.PC.De.B.1:** Controls are in place to restrict the use of removable media to authorized personnel. **D3.PC.Im.E.3:** Technical controls prevent unauthorized devices, including rogue wireless access devices and removable media from connecting to the internal network(s).
PR.PT-3: Access to systems and assets is controlled, incorporating the principle of least functionality. (p. 29)	**D3.PC.Am.B.7:** Access controls include password complexity and limits to password attempts and reuse. **D3.PC.Am.B.4:** User access reviews are performed periodically for all systems and applications based on the risk to the application or system. **D3.PC.Am.B.3:** Elevated privileges (e.g., administrator privileges) are limited and tightly controlled (e.g., assigned to individuals, not shared, and require stronger password controls). **D4.RM.Om.Int.1:** Third-party employee access to the institution's confidential data is tracked actively based on the principles of least privilege.
PR.PT-4: Communications networks are secured. (p. 29)	**D3.PC.Im.B.1:** Network perimeter defense tools (e.g., border router and firewall) are used. **D3.PC.Am.B.11:** Physical security controls are used to prevent unauthorized access to information systems, and telecommunication systems. **D3.PC.Im.Int.1:** The enterprise network is segmented in multiple, separate trust/security zones with defense-in-depth strategies (e.g., logical network segmentation, hard backups, air-gapping) to mitigate attacks.
DE.AE-1: A baseline of network operations and expected data flows for users and systems is established and managed. (p. 30)	**D3.DC.Ev.B.1:** A normal network activity baseline is established. **D4.C.Co.B.4:** Data flow diagrams are in place and document information flow to external parties.
DE.AE-2: Detected events are analyzed to understand attack targets and methods. (p. 30)	**D5.IR.Pl.Int.4:** Lessons learned from real-life cyber risk incidents and attacks on the institution and other organizations are used to improve the institution’s risk mitigation capabilities and response plan.
DE.AE-3: Event data are aggregated and correlated from multiple sources and sensors. (p. 30)	**D3.DC.Ev.E.1:** A process is in place to correlate event information from multiple sources (e.g., network, application, or firewall).

NIST Cybersecurity Framework	FFIEC Cybersecurity Assessment Tool
DE.AE-4: Impact of event is determined. (p. 30)	**D5.IR.Te.E.1:** Recovery scenarios include plans to recover from data destruction, and impacts to data integrity, data loss, and system and data availability. **D5.ER.Es.E.1:** Criteria have been established for escalating cyber incidents or vulnerabilities to the board and senior management based on the potential impact and criticality of the risk. **D1.RM.RMP.A.4:** A process is in place to analyze the financial impact cyber incidents have on the institution's capital.
DE.AE-5: Incident alert thresholds are established. (p. 30)	**D5.DR.De.B.1:** Alert parameters are set for detecting information security incidents that prompt mitigating actions. **D3.DC.An.E.4:** Thresholds have been established to determine activity within logs that would warrant management response. **D3.DC.An.Int.3:** Tools actively monitor security logs for anomalous behavior and alert within established parameters.
DE.CM-1: The network is monitored to detect potential cybersecurity events. (p. 30)	**D3.DC.An.B.2:** Customer transactions generating anomalous activity alerts are monitored and reviewed. **D3.DC.An.B.3:** Logs of physical and/or logical access are reviewed following events.
DE.CM-2: The physical environment is monitored to detect potential cybersecurity events. (p. 30)	**D3.PC.Am.E.4:** Physical access to high-risk or confidential systems is restricted, logged, and unauthorized access is blocked. **D3.Dc.Ev.B.5:** The physical environment is monitored to detect potential unauthorized access.
DE.CM-3: Personnel activity is monitored to detect potential cybersecurity events. (p. 31)	**D3.DC.An.A.3:** A system is in place to monitor and analyze employee behavior (network use patterns, work hours, and known devices) to alert on anomalous activities.
DE.CM-4: Malicious code is detected. (p. 31)	**D3.DC.Th.B.2:** Antivirus and anti-malware tools are used to detect attacks.
DE.CM-5: Unauthorized mobile code is detected. (p. 31)	**D3.PC.De.E.5:** Antivirus and anti-malware tools are deployed on end-point devices (e.g., workstations, laptops, and mobile devices).
DE.CM-6: External service provider activity is monitored to detect potential cybersecurity events. (p. 31)	**D4.RM.Om.Int.1:** Third-party employee access to the institution's confidential data is tracked actively based on the principles of least privilege.
DE.CM-7: Monitoring for unauthorized personnel, connections, devices and software is performed. (p. 31)	**D3.DC.Ev.B.3:** Processes are in place to monitor for the presence of unauthorized users, devices, connections, and software.

NIST Cybersecurity Framework	FFIEC Cybersecurity Assessment Tool
DE.CM-8: Vulnerability scans are performed. (p. 31)	**D3.DC.Th.E.5:** Vulnerability scanning is conducted and analyzed before deployment/redeployment of new/existing devices.
DE.DP-1: Roles and responsibilities for detection are well defined to ensure accountability. (p. 31)	**D3.DC.Ev.B.4:** Responsibilities for monitoring and reporting suspicious systems activity have been assigned.
DE.DP-2: Detection activities comply with all applicable requirements. (p. 32)	**D1.G.Ov.E.2:** Management is responsible for ensuring compliance with legal and regulatory requirements related to cybersecurity.
DE.DP-3: Detection processes are tested. (p. 32)	**D3.DC.Ev.Int.2:** Event detection processes are proven reliable.
DE.DP-4: Event detection information is communicated to appropriate parties. (p. 32)	**D3.DC.Ev.B.2:** Mechanisms (e.g., antivirus alerts, log event alerts) are in place to alert management to potential attacks. **D5.ER.Is.B.1:** A process exists to contact personnel who are responsible for analyzing and responding to an incident. **D5.ER.Is.E.1:** Criteria have been established for escalating cyber incidents or vulnerabilities to the board and senior management based on the potential impact and criticality of the risk.
DE.DP-5: Detection processes are continuously improved. (p. 32)	**D5.IR.Pl.Int.3:** Lessons learned from real-life cyber incidents and attacks on the institution and other organizations are used to improve the institution's risk mitigation capabilities and response plan.
RS.PL-1: Response plan is executed during or after an event. (p. 33)	**D5.IR.Pl.B.1:** The institution has documented how it will react and respond to cyber incidents.
RS.CO-1: Personnel know their roles and order of operations when a response is needed. (p. 33)	**D5.IR.Pl.B.3:** Roles and responsibilities for incident response team members are defined.
RS.CO-2: Events are reported consistent with established criteria. (p. 33)	**D5.IR.Pl.B.2:** Communication channels exist to provide employees a means for reporting information security events in a timely manner. **D5.DR.Re.B.4:** Incidents are classified, logged and tracked. **D5.DR.Re.E.6:** Records are generated to support incident investigation and mitigation. **D5.ER.Es.B.4:** Incidents are detected in real time through automated processes that include instant alerts to appropriate personnel who can respond.
RS.CO-3: Information is shared consistent with established criteria. (p. 33)	**D5.ER.Es.B.2:** Procedures exist to notify customers, regulators, and law enforcement as required or necessary when the institution becomes aware of an incident involving the unauthorized access to or use of sensitive customer information.

NIST Cybersecurity Framework	FFIEC Cybersecurity Assessment Tool
RS.CO-4: Coordination with stakeholders occurs consistent with response plans. (p. 33)	**D5.ER.Is.B.1:** A process exists to contact personnel who are responsible for analyzing and responding to an incident. **D5.IR.Pl.Int.1:** A strategy is in place to coordinate and communicate with internal and external stakeholders during or following a cyber attack.
RS.CO-5: Voluntary information sharing occurs with external stakeholders to achieve broader cybersecurity situational awareness. (p. 33)	**D2.IS.Is.B.3:** Information about threats is shared with law enforcement and regulators when required or prompted. **D2.IS.Is.E.2:** A representative from the institution participates in law enforcement or information-sharing organization meetings.
RS.AN-1: Notifications from the detection system are investigated. (p. 33)	**D5.DR.De.B.3:** Tools and processes are in place to detect, alert, and trigger the incident response program. **D5.DR.De.Int.3:** Incidents are detected in real time through automated processes that include instant alerts to appropriate personnel who can respond.
RS.AN-2: The impact of the incident is understood. (p. 34)	**D1.RM.RMP.A.4:** A process is in place to analyze the financial impact cyber incidents have on the institution's capital. **D5.IR.Te.E.1:** Recovery scenarios include plans to recover from data destruction, impacts to data integrity, data loss, and system and data availability. **D5.ER.Es.E.1:** Criteria have been established for escalating cyber incidents or vulnerabilities to the board and senior management based on the potential impact and criticality of the risk.
RS.AN-3: Forensics are performed. (p. 34)	**D3.CC.Re.Int.3:** Security investigations, forensic analysis, and remediation are performed by qualified staff or third parties. **D3.CC.Re.Int.4:** Generally accepted and appropriate forensic procedures, including chain of custody, are used to gather and present evidence to support potential legal action.
RS.AN-4: Incidents are categorized consistent with response plans. (p. 34)	**D5.ER.Es.B.4:** Incidents are classified, logged and tracked. **D5.DR.Re.E.1:** The incident response plan is designed to prioritize incidents, enabling a rapid response for significant cybersecurity incidents or vulnerabilities.

NIST Cybersecurity Framework	FFIEC Cybersecurity Assessment Tool
RS.MI-1: Incidents are contained. (p. 34)	**D.5.DR.Re.B.1:** Appropriate steps are taken to contain and control an incident to prevent further unauthorized access to or use of customer information. **D5.DR.Re.E.4:** Procedures include containment strategies and notifying potentially impacted third parties. **D5.DR.Re.E.2:** A process is in place to help contain incidents and restore operations with minimal service disruption. **D5.DR.Re.E.3:** Containment and mitigation strategies are developed for multiple incident types (e.g., DDoS, malware).
RS.MI-2: Incidents are mitigated. (p. 34)	**D5.DR.De.B.1:** Alert parameters are set for detecting information security incidents that prompt mitigating actions. **D5.DR.Re.E.3:** Containment and mitigation strategies are developed for multiple incident types (e.g., DDoS, malware). **D3.PC.Im.E.4:** A risk-based solution is in place at the institution or Internet-hosting provider to mitigate disruptive cyber attacks (e.g., DDoS attacks).
RS.MI-3: Newly identified vulnerabilities are documented as accepted risks. (p. 34)	**D1.RM.RA.E.1:** Risk assessments are used to identify the cybersecurity risks stemming from new products, services, or relationships.
RS.IM-1: Response plans incorporate lessons learned. (p. 34)	**D5.IR.Pl.Int.4:** Lessons learned from real-life cyber incidents and attacks on the institution and other organizations are used to improve the institution's risk mitigation capabilities and response plan.
RS.IM-2: Response strategies are updated. (p. 34)	**D5.IR.Pl.Int.4:** Lessons learned from real-life cyber incidents and attacks on the institution and other organizations are used to improve the institution's risk mitigation capabilities and response plan. **D5.IR.Te.Int.5:** The results of cyber event exercises are used to improve the incident response plan and automated triggers.
RC.RP-1: Recovery plan is executed during or after an event. (p. 34)	**D5.IR.Pl.B.6:** The institution plans to use business continuity, disaster recovery, and data backup programs to recover operations following an incident.
RC.IM-1: Recovery plans incorporate lessons learned. (p. 35)	**D5.IR.Pl.Int.4:** Lessons learned from real-life cyber incidents and attacks on the institution and other organizations are used to improve the institution's risk mitigation capabilities and response plan.

NIST Cybersecurity Framework	FFIEC Cybersecurity Assessment Tool
RC.IM-2: Recovery strategies are updated. (p. 35)	**D5.IR.Pl.Int.4:** Lessons learned from real-life cyber incidents and attacks on the institution and other organizations are used to improve the institution's risk mitigation capabilities and response plan. **D5.IR.Te.Int.5:** The results of cyber event exercises are used to improve the incident response plan and automated triggers.
RC.CO-1: Public Relations are managed. (p. 35)	**D5.ER.Es.Int.3:** An external communication plan is used for notifying media regarding incidents when applicable.
RC.CO-2: Reputation after an event is repaired. (p. 35)	**D5.IR.Pl.Int.1:** A strategy is in place to coordinate and communicate with internal and external stakeholders during or following a cyber attack.
RC.CO-3: Recovery activities are communicated to internal stakeholders and executive and management teams. (p. 35)	**D5.ER.Is.B.1:** A process exists to contact personnel who are responsible for analyzing and responding to an incident. **D5.IR.Pl.Int.1:** A strategy is in place to coordinate and communicate with internal and external stakeholders during or following a cyber attack.

Explanation of Cybersecurity Assessment Tool References

To reference the Cybersecurity Assessment Tool declarative statements, each has a unique identifier that comprises the Domain, Assessment Factor, Component, Maturity Level, and statement number. Each portion is separated by a period.

The following table provides the codes used in the above references for the Cybersecurity Assessment Tool. For example, "D1.G.Ov.B.1" refers to Domain: 1, Assessment Factor: Governance, Component: Oversight, Maturity Level: Baseline, and statement 1.

Domain	Assessment Factor	Component	Maturity Level
Domain 1: Cyber Risk Management and Oversight (D1)	Governance (G)	Oversight (Ov)	Baseline (B) Evolving (E) Intermediate (Int) Advanced (A) Innovative (Inn)
		Strategy/Policies (SP)	
		IT Asset Management (IT)	
	Risk Management (RM)	Risk Management Program (RMP)	
		Risk Assessment (RA)	
		Audit (Au)	
	Resources (R)	Staffing (St)	
	Training and Culture (TC)	Training (Tr)	
		Culture (Cu)	
Domain 2: Threat Intelligence and Collaboration (D2)	Threat Intelligence (TI)	Threat Intelligence and Information (Ti)	
	Monitoring and Analyzing (MA)	Monitoring and Analyzing (Ma)	
	Information Sharing (IS)	Informational Sharing (Is)	
Domain 3: Cybersecurity Controls (D3)	Preventative Controls (PC)	Infrastructure Management (Im)	
		Access and Data Management (Am)	
		Device/End-Point Security (De)	
		Secure Coding (Se)	
	Detective Controls (DC)	Threat and Vulnerability Detection (Th)	
		Anomalous Activity (An)	
		Event Detection (Ev)	
	Corrective Controls (CC)	Patch Management (Pa)	

Domain	Assessment Factor	Component	Maturity Level
		Remediation (Re)	
Domain 4: External Dependency Management (D4)	Connections (C)	Connections (Co)	
	Relationship Management (RM)	Due Diligence (Dd)	
		Contracts (Co)	
		Ongoing Monitoring (Om)	
Domain 5: Cyber Incident Management and Resilience (D5)	Incident Resilience Planning and Strategy (IR)	Planning (Pl)	
		Testing (Te)	
	Detection, Response and Mitigation (DR)	Detection (De)	
		Response and Mitigation (Re)	
	Escalation and Reporting (ER)	Escalation and Reporting (Es)	